Homework 5

MATH 301/601

Solutions to Graded Problems

Exercise 3. Suppose H is a nonempty finite subset of a group G and that H is closed under multiplication (that is, $ab \in H$ for all $a, b \in H$). Prove that H is a subgroup of G.

Solution. As H is closed under multiplication, it is enough to show that H contains the identity of G and that H is closed under inversion. We know H is nonempty, so let $h \in H$. Using the fact that H is finite, we can find $j, k \in \mathbb{Z}$ such that $j < k$ and $h^j = h^k$. It follows that $h^{k-j} = e$. Now, as H is closed under multiplication and $k - j \in \mathbb{N}$, we have that $e = h^{k-j} \in H$. Also, observe that $h^{k-j-1} = h^{-1}$, and as $k - j - 1 \in \mathbb{N} \cup \{0\}$, we have that $h^{-1} \in H$. As h was an arbitrary element of H, we see that H is closed under taking inverses. Therefore, H is a subgroup of G. □

Exercise 6. Suppose G is a nontrivial group in which the only two subgroups of G are itself and the trivial subgroup.

(a) Prove that G is cyclic.

(b) Using part (a), prove that G is a finite group of prime order.

Solution. (a) As G is nontrivial, there exists $g \in G \setminus \{e\}$. Since g is not the identity, the cyclic subgroup generated by g is nontrivial, and hence, as G has only two subgroups, the cyclic subgroup generated by g must be all of G. Therefore, G is cyclic. In fact, we have shown that every element of $G \setminus \{e\}$ is a generator of G.

(b) We have already established that G is cyclic, so we may choose a generator of G, call it a. If $a^2 = e$, then $|G| = 2$, and hence G is a finite group of prime order. We can therefore assume that $a^2 \neq e$, and hence, the cyclic subgroup generated by a^2 is equal to G. Therefore, there exists $k \in \mathbb{Z}$ such that $(a^2)^k = a$, which implies that $a^{2k-1} = e$. Hence, G has finite order.

Now, suppose that $n \in \mathbb{N} \setminus \{1\}$ divides $|G|$. We want to show that $n = |G|$. Let $q \in \mathbb{Z}$ such that $|G| = nq$. As $n > 1$, we must have that $q < |G|$; hence, $a^q \neq e$ and $|a^q| = |G|$. But, $(a^q)^n = (a^{qn}) = a^{|G|} = e$, which implies that $n \geq |G|$. Therefore, as $n \mid |G|$, we must have that $n = |G|$. We have shown that the only divisors of $|G|$ are 1 and itself, and so $|G|$ is prime. □